The Active Learning Trust

DATA SHARING POLICY

Personal Data

This policy is reviewed every two years

History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	DPO	June 2018	12 July 2018	1st formal issue
2	DPO	December 2018	13 December 2018	Minor amendment 4.3
3	DPO	May 2019	23 May 2019	Inclusion of exemptions

1. INTRODUCTION

1.1 The work of the Active Learning Trust ("Trust") requires the sharing of personal data and sometimes sensitive personal data between staff, between staff and students, and between staff and external third parties. It is important to ensure that such information is managed in a secure way at all times.

2. PURPOSE OF THE POLICY

2.1 This Policy aims to minimise the risk of loss, unauthorised disclosure, modification or removal of personal data maintained by the Trust.

2.2 This Policy is based on the Information Commissioner's Office (ICO) statutory code of practice for data sharing, available at ICO Data Sharing Code of Practice. Such Code has not yet been updated to reflect the General Data Protection Regulation ("GDPR"). The ICO is intending to revise this guidance in due course. It is also based on the ICO's Report of Data Protection Guidance it provided schools in 2012 - Data Protection Guidance 2012

3. SCOPE

3.1 This Data Sharing Policy ("Policy") is intended for all individuals and third parties who have access to the Trust's information and applies to Personal Data as defined in point 5 below.

4. RESPONSIBILITIES

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted and adhered to and is responsible for the day to day management of personal data sharing arrangements. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central Trust.

4.3 An Information Governance Working Group reports to the Trust's Senior Leadership Team and considers Trust wide information governance matters.

4.4 The Trust's Data Protection Officer is responsible for monitoring the Trust's compliance with the Policy.

5. PERSONAL DATA

5.1 Data in this Policy covers 'Personal Data' which is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1] such as a name, date of birth, address, NI number, medical information, exam results and an online identifier, such as an IP address.

5.2 A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

5.2.1 race or ethnic origin;
5.2.2 political opinions;
5.2.3 religious or philosophical beliefs;
5.2.4 trade union membership;
5.2.5 physical or mental health;
5.2.6 an individual's sex life or sexual orientation; and
5.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

5.3 Special Category Data is given special protection and additional safeguards apply if this information is to be collected and used.

5.4 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

6. DEFINITION OF DATA SHARING

6.1 The ICO defines "data sharing" as the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

6.1.1 a reciprocal exchange of data;
6.1.2 one or more organisations providing data to a third party or parties;
6.1.3 several organisations pooling information and making it available to each other;
6.1.4 several organisations pooling information and making it available to a third party or parties;
6.1.5 exceptional, one-off disclosures of data in unexpected or emergency situations; or
6.1.6 different parts of the same organisation making data available to each other.

6.2 There are two types of data sharing:

6.2.1 systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and

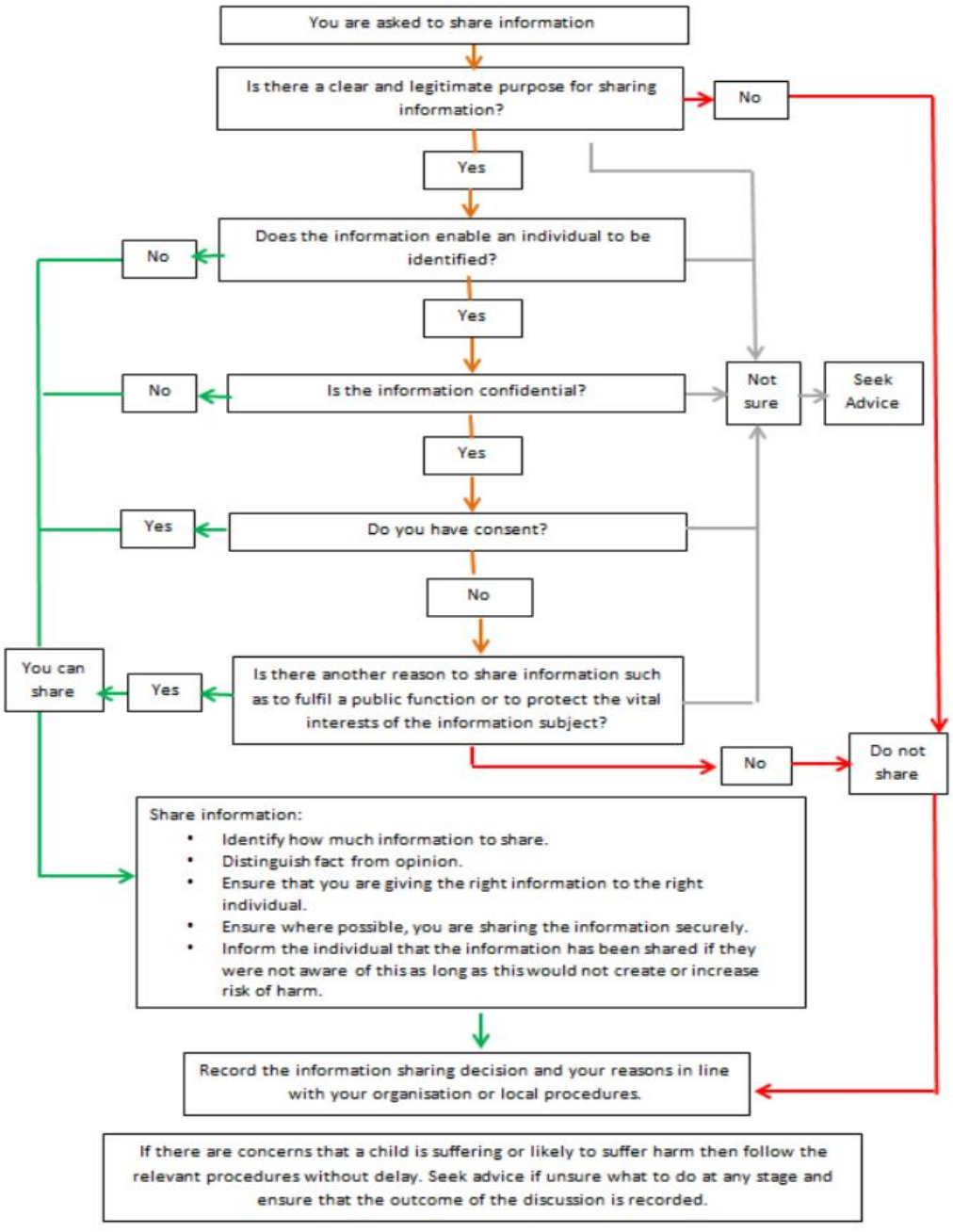
6.2.2 exceptional, one-off decisions to share data for any of a range of purposes.

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

6.3 Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither the Data Protection Act 2018 or General Data Protection Regulation 2018 apply to that type of sharing.

7. DECIDING TO SHARE PERSONAL DATA

7.1 When deciding whether to enter into an arrangement to share personal data (either as a provider, a recipient or both) a person needs to identify the objective that it is meant to achieve (refer chart below and Appendices I and II.) A Data Protection Impact Assessment ("DPIA") requires to be undertaken to assess the potential benefits and risks to individuals or society, of sharing the personal data. The results of not sharing the personal data should be assessed and recorded.



7.2 The following questions should be considered as part of the DPIA:

7.2.1 *What is the sharing meant to achieve?* There should be a clear objective or set of objectives. Being clear about this will allow a person to work out what data needs to be shared and who with. It is good practice to document this.

7.2.2 *What information needs to be shared?* All the personal data held about someone should not be shared if only certain data items are needed to achieve a person's objectives. For example, there might be a need to share somebody's current name and address, but not other information held about them.

7.2.3 *Who requires access to the shared personal data?* The 'need to know' principles should be considered, meaning that other organisations should only have access to personal data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

7.2.4 *When should it be shared*? It is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

7.2.5 *How should it be shared?* This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

7.2.6 *How can checks be made that the sharing is achieving its objectives?* Judgement will be needed as to whether it is still appropriate and confirm that the safeguards still match the risks.

7.2.7 *What risk does the data sharing pose?* For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

7.2.8 *Could the objective be achieved without sharing the data or by anonymising it*? It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

7.2.9 *Will any of the personal data be transferred outside of the European Economic Area (EEA) and if so whether the security mechanisms are in place*. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.3 In all circumstances of information sharing, staff will ensure that:

7.3.1 When information needs to be shared, sharing complies with the law, guidance and best practice;

7.3.2 Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the contract explicitly permits it;

7.3.3 Individuals' rights will be respected, particularly confidentiality and security;

7.3.4 Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure; and

7.3.5 Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations.

7.4 Any new information assets and data flows that arise out of a new project or procurement or process where the Trust is the data controller or receives personal, confidential, sensitive personal data, will need to be recorded in a school's Information Asset Register.

7.5 Some information sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared. Refer to the Information Commissioner's Office (ICO) anonymisation code of practice for further information - ICO Anonymisation Code of Practice

8. DATA SHARING AGREEMENTS

8.1 Data sharing agreements, sometimes known as 'information sharing agreements', set out a common set of rules to be adopted by the various organisations involved in an information sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

8.2 A data sharing agreement must, at least, document the following:

8.2.1 the purpose, or purposes, of the sharing;
8.2.2 the legal basis for sharing;
8.2.3 the potential recipients or types of recipient and the circumstances in which they will have access;
8.2.4 who the data controller(s) is and any data processor(s);
8.2.5 the personal data to be shared;
8.2.6 data quality – accuracy, relevance, usability;
8.2.7 data security;
8.2.8 retention of shared data;
8.2.9 individuals' rights – procedures for dealing with access requests, queries and complaints;
8.2.10 review of effectiveness/termination of the sharing agreement;

8.2.11 any particular obligations on all parties to the agreement, giving an assurance around the standards expected; and

8.2.12 sanctions for failure to comply with the agreement or breaches by individual staff.

8.3 A Data Sharing Register ("Register") will be maintained by each school which records the data sharing agreements which a school has entered into. This allows the register to be monitored to ensure that the partnerships and agreements are current and remain effective.

9. DATA SHARING WITHIN A SCHOOL

9.1 Schools need to consider the following six data protection principles as laid down in the GDPR are followed at all times, even when sharing information within their own organisations, or between members of staff:

9.1.1 personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

9.1.2 personal data shall be collected for legitimate purposes and shall not be further processed in a manner incompatible with those purposes;

9.1.3 personal data shall be adequate, relevant, and limited to what is necessary for the purposes(s) for which it is being processed;

9.1.4 personal data shall be accurate and, where necessary, kept up to date;

9.1.5 personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose/those purposes; and

9.1.6 personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

9.2 Staff should only have access to personal data and special categories of personal data also known as sensitive personal data if they require the information to carry out their duties. Security mechanisms to ensure that only appropriate access is permitted to personal data is covered in the section 11 titled "User Privilege Management" of the Trust's ICT Security Policy.

10. DATA SHARING WITHIN THE MULTI ACADEMY TRUST

10.1 The Trust and its constituent schools must ensure that any personal data shared between schools in the Trust and a school and the Trust must be processed fairly and lawfully. Schools and the Trust will be clear and transparent with individuals about how their information is processed and ensure that it falls within their expectations. The Trust is included in each school's privacy notice as an organisation where personal data may be shared.

11. PRIVACY NOTICE

11.1 The Data Protection Act 2018 requires that personal data be processed fairly. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for. In a broader sense, fairness also requires that where personal data is shared, this happens in a way that is reasonable, and that people would be likely to expect and would not reasonably object to if given the chance. This needs to be considered before any personal data is shared. This applies equally to routine data sharing or a single, one-off disclosure.

11.2 Five types of privacy notices (formerly called fair processing notices) are issued by the Trust which informs people how the Trust and its schools process personal data:

11.2.1 Workforce Privacy Notice
11.2.2 Pupils (also provided to parents and carers) Privacy Notice
11.2.3 Trustees, Governors and Volunteers Privacy Notice
11.2.4 Job Applicants Privacy Notice
11.2.5 Suppliers Privacy Notice

11.3 In a data sharing context, a privacy notice should at least tell the individual:

11.3.1 who is the organisation
11.3.2 why personal data may be shared
11.3.3 who personal information is to be shared with – this could be actual named organisations or types of organisation.

12. SECURITY

12.1 The following measures should be taken in respect of information that schools share with other organisations, or that other organisations share with schools:

12.1.1 Review what personal data a school receives from other organisations, making sure the origin is known and whether any conditions are attached to its use;

12.1.2 Review what personal data a school shares with other organisations, know who has access is it and what it will be used for;

12.1.3 Assess whether any data shared is particularly sensitive (special category personal information) and afford this data a suitably high level of security;

12.1.4 Identify who has access to information that other organisations have shared with a school; ‘need to know’ principles should be adopted. Schools should avoid giving all their staff access to shared information if only a few of them need it to carry out their job;

12.1.5 Consider the effect a security breach could have on individuals;

12.1.6 Consider the effect a security breach could have on the Trust in terms of cost, reputational damage or lack of trust from employees, parents and

carers. This can be particularly acute where an individual provides their personal data to the Trust, but a third-party recipient organisation then loses the data. Schools should aim to build a culture within a school where employees know and understand good practice, in respect of 'its own' data and that received from another organisation.

12.2 Staff should be aware of security policies and procedures and be trained in their application. In particular schools will need to:

12.2.1 design and organise security to fit the type of personal data disclosed or received and the harm that may result from a security breach;

12.2.2 be clear about which staff members in schools involved in the sharing are responsible for ensuring information security. They should meet regularly to ensure appropriate security is maintained;

12.2.3 have appropriate monitoring and auditing procedures in place; and

12.2.4 be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively.

Physical Security	**Technical Security**
Does a school have good quality access control systems to its premises?	Is technical security appropriate to the type of system, type of information held and what is done with it?
How are visitors supervised?	If staff work at home are security measures in place to ensure that this does not compromise security?
Is paper based information stored and transferred securely?	How is encryption of personal data implemented and managed?
Are laptops and removable media locked away at night either in the school or at an employee's home?	Have the most common security risks associated with using a web-product been identified e.g. a website, web application or mobile application?
Is paper waste disposed of securely?	How is access to school systems controlled?
	Are privileges set to information based on people's need to know?
	What measures are in place for the security of information in transit?

13. PROTECTION OF THIRD PARTIES – EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS

13.1 The GDPR and the Data Protection Act 2018 set out exemptions from some of the rights and obligations in some circumstances. Exemptions should not routinely relied upon and should be considered on a case-by-case basis. The main ones which are detailed in the Trust's SAR guidance and apply to schools are:

- Confidential references

- Negotiations between Employer and Employee - the release of the data would prejudice the negotiations

- Management Forecasting/planning - and its release to an individual would prejudice the Trust's business or activities

- Complaints
- Legal professional privilege
- Exam Scripts and Marks – this excludes an examiner's comments
- Preventing and Detecting crime – the release of the data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders

- Health Data - Serious Harm Test - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services

- Education Data – Serious Harm

- Child Abuse Data - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services.

13.2 Where personal data is not to be provided due to application of an exemption, a school should ensure it internally documents its reasoning for withholding this data. The personal data withheld and exemption applied should also be recorded in the Trust's SAR Log.

14. DATA STANDARDS

14.1 Procedures should be in place to maintain the quality of the personal data a school holds, especially when it intends to share data. When a school is planning to share data with another organisation, it needs to consider all the data quality implications.

14.2 When sharing information, a school should consider the following issues:

14.2.1 Make sure that the format of the data shared by schools is compatible with the systems used by both organisations;

14.2.2 Check that the information shared is accurate before it is shared;

14.2.3 Establish ways for making sure inaccurate data is corrected by all the organisations holding it; and

14.2.4 Agree common retention periods and deletion arrangements for the data sent and received.

15. REVIEW OF DATA SHARING AGREEMENTS

15.1 Data sharing agreements should be reviewed on a regular basis as changes can occur and schools need to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

15.2 Key questions that should regularly be asked:

15.2.1 Is the personal data still needed?

15.2.2 Do privacy notices and any data sharing agreements in place accurately explain the data sharing being carried out?

15.2.3 Are information governance procedures still adequate and working in practice?

15.2.4 Are people still entitled to access all the information?

15.2.5 Have people's queries and complaints being responded to properly and are they being analysed to make improvements to data sharing arrangements?

16. THINGS TO AVOID

16.1 When sharing personal data there are some practices that should be avoided. These practices could lead to regulatory action:

16.1.1 Misleading individuals about whether their information will be shared. For example, not telling individuals that their personal data will be shared as they may object;

16.1.2 Sharing excessive or irrelevant information about individuals. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is being shared for;

16.1.3 Sharing personal data when there is no need to do so – for example where anonymised statistical information can be used to plan service provision;

16.1.4 Not taking reasonable steps to ensure that information is accurate and up to date before it is shared. For example, failing to update address details before sharing information, leading to individuals being pursued at the wrong address or missing out on important information;

16.1.5 Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data; and

16.1.6 Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal details. For example, sending personal data

between organisations on an unencrypted USB memory stick which is then lost or faxing sensitive personal data to a general office number.

17. NOTIFICATION

17.1 The Data Protection Act requires that organisations provide the ICO with a description of the individuals or organisations to whom they intend or may wish to disclose personal data. The legal requirement is to provide a description of the recipient or the recipients of the data i.e. the types of organisation, not the names of specific organisations. The notification requirement does not include people to whom an organisation may be required by law to disclose personal data in a particular case, for example where the police require a disclosure of personal data under a warrant.

17.2 When personal data will be shared with another organisation or group of organisations the notification held with the ICO must be checked to ascertain if it needs to be updated. When any part of the notification entry becomes inaccurate or incomplete, for example because disclosure of personal information is being made to a new type of organisation, the ICO must be informed as soon as practical and in any event within 28 days. It is a criminal offence not to do this.

18. FREEDOM OF INFORMATION

18.1 The Freedom of Information Act 2000 ("FOIA") gives everyone the right to ask for information held by a public authority and, unless exempt, to be told whether the information is held and to be provided with the information.

18.2 The FOIA requires every public authority to adopt and maintain a publication scheme, which is a commitment to publish information on a proactive and routine basis. This supports the culture of transparency introduced by freedom of information legislation and allows the public to easily identify and access a wide range of information without having to make a request.

18.3 The Trust has a Freedom of Information Policy and Publication Scheme which are held on its website.

19. FURTHER ADVICE

19.1 With information sharing there may be exceptional and difficult circumstances where advice may be needed. The Trust's Data Protection Officer should be consulted where there are any concerns about whether the proposed information sharing is appropriate.

20. TRAINING

20.1 Staff should be trained so that they know who has the authority to share personal data, and in what circumstances this can take place.

20.2 The focus of the training should be enabling staff to make informed decisions about whether or how to share data, and how to treat the data they are responsible for.

20.3 People who have overall responsibility for data sharing need to be aware of:

20.3.1 the relevant law surrounding data sharing, including the Data Protection Act;

20.3.2 any relevant professional guidance or ethical rules;

20.3.3 data sharing agreements and the need to review them;

20.3.4 how different information systems work together;

20.3.5 security and authorising access to systems holding shared data;

20.3.6 how to conduct data quality checks; and

20.3.7 retention periods for shared data.

They also need the seniority and influence to make authoritative decisions about data sharing.

21. REPORTING

21.1 The Trust's Data Protection Officer is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on an annual basis.

22. REVIEW

22.1 This Policy will be reviewed every two years by the Trust Board.

APPENDIX I

DATA SHARING AGREEMENT CHECKLIST

Things to consider if/when a school wants to enter into an agreement to share personal data in "one-off" circumstances.

Is the Sharing Justified? - Key points to consider

- Do you think you should share the personal information?
- Have the potential benefits/risks to individuals/society of sharing/not sharing been assessed?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the Data Protection Act to share?

Do you have Power to Share? - Key points to consider

- The nature of the information you have been asked to share (e.g. was is it given in confidence?)
- Any legal obligation to share information (e.g. a statutory requirement or a court order)

If you decide to share – Key points to consider

- What information do you need to share? (only share what is necessary / distinguish fact from opinion)
- How should the information be shared? (must be sent securely & provided to the right person)
- Consider whether it is appropriate/ safe to inform the individual that you have shared their information

Record Your Data Sharing Decision & Reasoning

- What information was shared and for what purpose?
- Who was it shared with and when?
- The justification for sharing
- Whether the information was shared with or without consent

If you have any queries on Data Sharing, please contact your Headteacher or email the Trust's Data Protection Officer at Dataprotection@activelearningtrust.org

APPENDIX II

DATA SHARING AGREEMENT CHECKLIST

Things to consider if/when a school wants to enter into an agreement to share personal data on an ongoing basis.

Is the Sharing Justified? - Key points to consider

- What is the sharing meant to achieve?
- Have the potential benefits/risks to individuals/society of sharing/not sharing been assessed?
- Is the sharing proportionate to the issue being addressed?
- Could the objective be achieved without sharing personal data?

Do you have Power to Share? - Key points to consider

- The nature of the information you have been asked to share (e.g. was is it given in confidence?)
- Any legal obligation to share information (e.g. a statutory requirement or a court order)

If you decide to share – include the following in the Data Sharing Agreement

- What information needs to be shared
- The organisations that will be involved
- What you need to tell people about the data sharing and how you will communicate that information
- Measures to ensure adequate security is in place to protect the data
- What arrangements need to be in place to provide individuals with access to their personal data if they request it
- Agreed common retention periods for the data
- Processes to ensure secure deletion takes place

If you have any queries on Data Sharing, please contact your Headteacher or email the Trust's Data Protection Officer at Dataprotection@activelearningtrust.org